SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT

40 Rector Street, 9th Floor
New York, New York 10006
www.StopSpying.org | (212) 518-7573

STATEMENT OF
ALBERT FOX CAHN, EXECUTIVE DIRECTOR
AND NINA LOSHKAJIAN, STAFF ATTORNEY
SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT ("S.T.O.P.")

BEFORE THE COMMITTEES ON PUBLIC SAFETY AND TECHNOLOGY,
NEW YORK CITY COUNCIL

FOR AN OVERSIGHT HEARING ON NYPD'S IMPLEMENTATION OF THE PUBLIC OVERSIGHT OF SURVEILLANCE TECHNOLOGY (POST) ACT

PRESENTED
December 15th, 2023

Good morning, Chair Gutiérrez, Chair Hanks, and members of the Committees on Technology and Public Safety. The Surveillance Technology Oversight Project ("S.T.O.P.") is a New York-based civil rights and anti-surveillance group that advocates and litigates against discriminatory surveillance. Thank you for organizing this important hearing. We urge the Council to make NYPD surveillance reporting requirements enforceable and to ban police use of the most dangerous tools of police surveillance, including biased and ineffective facial recognition technology (FRT).

I. History of the POST Act and NYPD's Noncompliance

The Public Oversight of Surveillance Technology (POST) Act, enacted in 2020, was the first New York City surveillance law since 9/11, and it required the NYPD to detail every technology it uses and how NYPD data is shared.[1] The law came in response to widespread outrage over the ineffectiveness, invasiveness, and cost of NYPD's growing surveillance arsenal. Prior to the POST Act, the NYPD attempted to hide its use of invasive and creepy tools including StingRays, which mimic cellphone towers,[2] social media monitoring, Wi-Fi-based location tracking, the Domain Awareness System, and much more.[3] Though the POST Act only required minimal transparency, that didn't stop then-NYPD Deputy Commissioner from decrying the effort as "insane" and claiming the oversight law would become an "invaluable roadmap to criminals, terrorists, and others for how to harm the public."[4] Clearly, this has not been the reality, but the NYPD will continue to say that the sky is falling whenever it is held to even the lowest standard of accountability.

In reality, the importance of oversight of NYPD surveillance is indispensable given the Department's sustained discrimination against BIPOC communities, Muslim New Yorkers, and LGBTQ+ New Yorkers. Surveillance technology amplifies historical policing biases, systematically surveilling low-income communities of color.[5] Partnering with Amnesty International, we found: "the higher the proportion of non-white residents, the higher the concentration of facial recognition compatible CCTV cameras."[6]

Thanks to the POST Act, billions of dollars in NYPD surveillance contracts previously hidden under the Special Expenses program were brought to light.[7] The controversial secrecy agreement was terminated in 2020 in direct response to the POST Act's passage. Working with the Legal Aid Society, we demanded the New York City Comptroller reveal records from the program and have exposed

---

[1] Public Oversight of Surveillance Technology (POST) Act, N.Y. CITY COUNCIL § 14-188 (N.Y. 2017), https://legistar.council.nyc.gov/LegislationDetail.aspx?ID=3343878&GUID=996ABB2A-9F4C-4A32-B081-D6F24AB954A0.
[2] *NYPD Has Used Stingrays More Than 1,000 Times Since 2008*, NYCLU, Feb. 11, 2016, https://www.nyclu.org/en/pressreleases/nypd-has-used-stingrays-more-1000-times-2008.
[3] Ayyan Zubair, *Domain Awareness System*, SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT, Sept. 26, 2019, https://www.stopspying.org/latest-news/2019/9/26/domain-awareness-system.
[4] Nathan Tempey, *Top NYPD Official: Subjecting Our Surveillance Tools to Public Scrutiny Would Be 'Insane',* GOTHAMIST, June 14, 2017, https://gothamist.com/news/top-nypd-official-subjecting-our-surveillance-tools-to-public-scrutiny-would-be-insane.
[5] Eleni Manis et al., *Scan City: A Decade of NYPD Facial Recognition Abuse*, SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT, July 8, 2018, https://www.stopspying.org/scan-city.
[6] *Inside the NYPD's Surveillance Machine*, AMNESTY INTERNATIONAL, https://banthescan.amnesty.org/decode.
[7] NYPD "Special Expenses" Contracts, Surveillance Technology Oversight Project, https://www.stopspying.org/nypd-special-expenses.

secret surveillance equipment that was hidden for more than a decade, including $400 million on the Domain Awareness System.[8]

The POST Act was an essential first step in gaining greater transparency over the state of surveillance in New York City, but the NYPD has blatantly disregarded the requirements it imposes. The law does not set a high bar: NYPD is only required to disclose its surveillance tools and data sharing policies. Still, the NYPD has failed to clear even the low bar set by the POST Act. It failed to comply with the law's reporting requirements with the draft "impact and use" policies published for public comment in January 2021, which consisted largely of boilerplate language not specific to each individual technology. NYPD then failed to respond to the public's requests for more information when it published its revised policies in April 2021.

The impact and use policies required from the NYPD under the POST Act were meant to help the public and lawmakers gain crucial information on the Department's surveillance practices. The consequences of NYPD's spying are far-reaching, and therefore it is impossible to protect our communities without real insight. For example, because of NYPD's secrecy, we don't know what data ICE can access through fusion centers and other data sharing agreements, meaning we can't ensure NYPD isn't putting undocumented New Yorkers at risk of detention or deportation. We don't know what private contractors get access to our info. And, terrifyingly, we don't know how much bias the NYPD thinks is acceptable in its tools of mass surveillance, an incredibly disturbing state of affairs given the NYPD's civil rights record.

Attached to this testimony as addendum A is a document containing S.T.O.P.'s organizational comments submitted to the NYPD in February 2021 in response to its initial publication of draft impact and use policies for public comment. These comments detail the lack of substance in the policies, including the lack of disclosure of vendors' names, incomplete information on who can access the NYPD's collected data, NYPD's failure to meaningfully address whether tools had a disparate impact on protected groups, and missing definitions of artificial intelligence and machine learning, and more. S.T.O.P. also joined a coalition of concerned organizations who submitted a letter to the NYPD arguing that its draft policies demonstrated the department had failed to make a good-faith effort to comply with the POST Act.[9] Unfortunately, when the NYPD published its revised policies in April 2021, they still fell short of the POST Act's minimal requirements.[10]

II. NYPD Falls Short of the Standards Set by Other U.S. Police Agencies

The NYPD has shown the most egregious violations of the laxest law. NYPD's failure to comply falls far short of the standards other U.S. police departments bound by similar measures have established. In our whitepaper titled "New CCOPS on the Beat: An Early Assessment of Community Control Over Police Surveillance Laws," we performed a systematic review of all the Community Control of

---

[8] *Id.*

[9] *Coalition of Advocates and Academics Submit Joint Comments Documenting the NYPD's Failure to Comply with the POST Act*, BRENNAN CENTER FOR JUSTICE, Feb. 24, 2021, https://www.brennancenter.org/our-work/research-reports/coalition-advocates-and-academics-submit-joint-comments-documenting-nypds.

[10] Eleni Manis and Albert Fox Cahn, Above *The Law?: NYPD Violations of the Public Oversight of Surveillance Technology (POST) Act*, SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT, Oct. 7, 2021, 6, https://static1.squarespace.com/static/5c1bfc7eee175995a4ceb638/t/615df7245561b315e7289cee/1633548068620/2021.10.7_Above+the+Law_Research+Report.pdf.

Police Surveillance (CCOPS) laws in the country, and NYPD boasted the worst compliance record in the face of the weakest statute.[11] With New York City as a significant outlier, the report showed that many jurisdictions have—at least to some extent—seen increased transparency about and control over local law enforcement use of surveillance technology after passing a CCOPS ordinance. We followed up on this review with another whitepaper titled "Above The Law?: NYPD Violations of the POST Act" which further illustrated how NYPD has flouted its legal obligations.

Specifically, the Seattle Police Department provides names of specific vendors and models of technology. The NYPD only does so in two of its impact and use policies.[12] The Berkeley Police Department discloses each of the vendors with which it shares data and the City Manager of Cambridge, Massachusetts prepares an Annual Surveillance Report to the City of Cambridge that identifies the city's surveillance technology vendors and the third-party entities with which it shares data collected by each technology.[13] The NYPD, by contrast, only vaguely states that "[v]endors and contractors may have access" to surveillance technology "associated with software or data in performance of contractual duties to the NYPD."[14] The Berkeley Police Department provides concrete data retention periods in its policies,[15] while the NYPD fails to provide specific timeframes in the majority of its policies.[16] The bar for the NYPD is so low and they still trip over it.

---

[11] *New CCOPS on the Beat: An Early Assessment of Community Control Over Police Surveillance Laws*, SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT & HOGAN LOVELLS, LLP, Feb. 10, 2021, https://www.stopspying.org/ccops.

[12] *See, e.g.*, Seattle Police Department, Forward Looking Infrared Real-Time Video (FLIR) (KCSO Helicopters), Seattle Information Tech. (2020), https://www.seattle.gov/Documents/Departments/Tech/Privacy/FLIR%20-%20KCSO%20Helicopters%20WG%20SIR.pdf (listing the specific models and makes of its helicopters); Seattle Police Department, Automated License Plate Recognition (ALPR) (Patrol), Seattle Information Tech. (Jan. 31, 2019), https://www.seattle.gov/Documents/Departments/Tech/Privacy/SPD%20ALPR%20(Patrol)%20-%20Final%20SIR.pdf (identifying vendor of software); Seattle Police Department, CopLogic, Seattle Information Tech. (2019), https://www.seattle.gov/Documents/Departments/Tech/Privacy/SPD%20CopLogic%20Final%20SIR.pdf (identifying specific software and vendor of surveillance technology).

[13] Annual Surveillance Report, City Of Cambridge (Feb. 28, 2020), https://www.cambridgema.gov/-/media/Files/citymanagersoffice/surveillanceordinancedocuments/secondannualsurveillancereports_combined22820.pdf.

[14] *See, e.g.*, Audio-Only Recording Devices, Covert: Impact and Use Policy, NYPD (Apr. 11, 2021), https://www1.nyc.gov/assets/nypd/downloads/pdf/public_information/post-final/audio-only-recording-devices-covert-nypd-- impact-and-use-policy_4.9.21_final.pdf.

[15] *See, e.g.*, Berkeley Police Department, Surveillance Use Policy – Body Worn Cameras, City of Berkeley (Feb. 25, 2021), https://www.cityofberkeley.info/uploadedFiles/Police/Level_3_-_General/Surveillance_Use_Policy_-_Body_Worn_Cameras.pdf.

[16] Closed circuit television systems, manned aircraft systems, and unmanned aircraft systems have a standard retention period of 30 days, subject to exception through the Retention and Disposition Schedule for New York Local Government Records. ClosedCircuit Television Systems: Impact and Use Policy, NYPD (Apr. 11, 2021), https://www1.nyc.gov/assets/nypd/downloads/pdf/public_information/post-final/cctv-systems-nypd-Impact-and-usepolicy_4.9.21_final.pdf; Manned Aircraft Systems: Impact and Use Policy, NYPD (Apr. 11, 2021), https://www1.nyc.gov/assets/nypd/downloads/pdf/public_information/post-final/manned-aircraft-systems-nypd-impact-and-usepolicy_4.9.21_final.pdf; Unmanned Aircraft Systems: Impact and Use Policy, NYPD (Apr. 11, 2021), https://www1.nyc.gov/assets/nypd/downloads/pdf/public_information/post-final/unmanned-aircraft-systems-uas-nypd-impactand-use-policy_4.9.21_final.pdf. ShotSpotter has a retention period of 30 hours, subject through the Retention and Disposition Schedule for New York Local Government Records. ShotSpotter: Impact and Use Policy, NYPD (Apr. 11, 2021), https://www1.nyc.gov/assets/nypd/downloads/pdf/public_information/post-final/shotspotter-nypd-impact-and-usepolicy_4.9.21_final.pdf. License plate readers have a standard retention rate of 5 years, subject to exception through the Retention and Disposition Schedule for New York Local Government Records. License Plate Readers: Impact and Use Policy, NYPD (Apr. 11, 2021),

III. OIG Report Proves NYPD's Noncompliance

The POST Act requires the Office of the Inspector General (OIG) for the NYPD to annually audit NYPD compliance. In 2022, more than two years after the law was enacted, the OIG finally published its audit.[17] The report detailed the NYPD's many shortcomings and urged the NYPD to give both the OIG and the public greater information about how New Yorkers are surveilled. Stunningly, the OIG stated very clearly that it believed NYPD's narrow interpretation of the POST Act undermines the law. Advocates and community members had been making this claim for years but, coming from another city agency, this was a landmark statement. Its other key findings were:

- NYPD used boilerplate language for its POST Act reports, hiding details of specific technologies;
- The NYPD largely failed to address the bias of its surveillance tools;
- The NYPD used blanket reports for multiple tools, once again detailed data for each technology; and
- NYPD failed to specify the specific safeguards / data sharing arrangements for each technology.[18]

In total, the OIG made fifteen specific and straightforward recommendations. The NYPD, however, only even considered implementing one—potentially issuing press releases when it publishes new impact and use policies—and rejected 93% of the advice in the OIG's report outright, according to the OIG's ninth Annual Report issued in March 2023.[19] The NYPD's blatant disregard for its obligations under the law makes it clear that the Council must take additional steps to rein in its abusive practices when it comes to surveillance technology.

IV. Need for Amendments and Bans on the Worst Police Surveillance

We urge the Council to listen to advocates and the OIG in taking urgent steps to ensure the NYPD follows the rule of law. Attached to this testimony as addendum B is a draft of legislation we support that would amend the POST Act to impose additional reporting and compliance requirements on the NYPD. This legislation can fix some of the loopholes the NYPD is currently exploiting, specifically by requiring a separate impact and use policy for each individual surveillance technology the department uses and the disclosure of which agencies have access to NYPD data. We also recommend the Council create a private right of action to make it clear that New Yorkers should have the right to sue the NYPD when they are violating the law.

This legislation would be crucial in creating some actual transparency and would also importantly alleviate the need for many ongoing lawsuits against the NYPD for its secrecy in using surveillance technology. Since the passage of the POST Act, we have filed nearly a dozen lawsuits stemming from

---

https://www1.nyc.gov/assets/nypd/downloads/pdf/public_information/post-final/license-plate-readerslpr-nypd-impact-and-use-policy_4.9.21_final.pdf.

[17] *An Assessment of NYPD's Response to the POST Act*, N.Y.C. DEP'T OF INVESTIGATION OFFICE OF THE INSPECTOR GENERAL FOR THE NYPD, Nov. 2022, https://www.nyc.gov/assets/doi/reports/pdf/2022/POSTActReport_Final_11032022.pdf.

[18] *Id.*

[19] *Ninth Annual Report*, N.Y.C. DEP'T OF INVESTIGATION OFFICE OF THE INSPECTOR GENERAL FOR THE NYPD, March 2023, 5, https://www.nyc.gov/assets/doi/reports/pdf/2023/13OIGNYPDRpt.Release.03.30.2023.pdf

public records requests made to the NYPD. These lawsuits would not be necessary were the NYPD actually in compliance with the POST Act. For example, we represent Amnesty International USA (AI USA) in its lawsuit seeking NYPD records on its surveillance of historic Black Lives Matter protests in the summer of 2020, specifically records concerning the procurement, functionality, and general use of FRT, drones, gait recognition, cell-site simulators, and ambient sound recording devices. This litigation would not be necessary if the NYPD impact and use policies actually disclosed useful and detailed information.

Further, even if we are going to have the best transparency bill, it will not enough on its own to rein in the NYPD. Given NYPD's obvious contempt for oversight in the three years since the POST Act's passage, the Council must go further and ban police use of broken, biased surveillance technology like facial recognition, the so-called 'gang database,' and others. There are certain systems whose bias and ineffectiveness is already so well-documented that no additional information from the NYPD would justify their continued use. One such system is facial recognition.

We urge the Council to introduce a ban on government use of FRT, and to support Intros 1014 and 1024 banning use of FRT in places of public accommodation and residences. FRT is biased and error prone. Systems can be up to 99% accurate for middle-aged white men under ideal lighting in laboratory conditions but can be wrong more than 1 in 3 times for some women of color, even under similar conditions.[20] Numerous people, disproportionately Black, are wrongly arrested after being misidentified through facial recognition.[21] Additionally, when facial recognition software can only recognize two genders, we leave transgender and non-binary individuals susceptible to misidentification and wrongful arrest.[22]

Intro 1014 specifically prohibits any place or provider of public accommodation from using any biometric recognition technology to verify or identify a customer. It also prohibits businesses from barring entry to customers based on FRT and prevents companies from selling customers biometric data. This would be a crucial step towards protecting New Yorkers and preventing the types of abuses of the technology that we are seeing in places of public accommodation like Madison Square Garden, where owner James Dolan has vindictively used the incredible power of FRT to seek vengeance against his foes, blocking access to ticketholders who are affiliated with law firms involved in pending lawsuits against his company.

Use of FRT in residential settings opens tenants to harassment, discriminatory eviction, and compromises their privacy. New Yorkers do not want this invasive technology used in their homes, the most intimate of spaces.[23] Intro 1024 would prohibit any owner of a multiple dwelling from installing, activating, or using any biometric recognition technology that identifies tenants or the guest

[20] Joy Buolamwini, Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification, Proceeds of Machine Learning Research*, vol 81, 1-15, 2018 p. 1.
[21] Kashmir Hill, *Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match*, N.Y. TIMES, Dec. 29, 2020, https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html.
[22] Rachel Mentz, *AI Software Defines People as Male or Female. That's a Problem*, CNN BUSINESS, Nov. 21, 2019, https://www.cnn.com/2019/11/21/tech/ai-gender-recognition-problem/index.html.
[23] Yasmin Gagne, *How We Fought Our Landlord's Secretive Plan for Facial Recognition—and Won*, Nov. 22, 2019, FAST COMPANY, https://www.fastcompany.com/90431686/our-landlord-wants-to-install-facial-recognition-in-our-homes-but-were-fighting-back.

of a tenant. The bill should be strengthened through amendments creating a strong private right of action applicable to all provisions, not just sale, with statutory damages and punitive damages, but its passage is critically important to make New Yorkers safer in their homes. Private FRT systems are just one 911 call away from being used by the NYPD, meaning these bills are also crucial to protect New Yorkers from false arrest and unwarranted police harassment.

A bill is urgently needed to ban police use of FRT as well. In this context, officers use pseudoscientific tactics that exacerbate the risk of error, such as running scans of celebrity lookalikes.[24] The Georgetown Law Center on Privacy and Technology documented the kinds of abuses that are "common practice" at NYPD.[25] One of the most egregious practices is that of routinely altering photos. The report revealed that NYPD edits of images "often go well beyond minor lighting adjustments and color correction," and in many instances "amount to fabricating completely new identity points not present in the original photo."[26] Police also abuse this tech to surveil protestors. There are reports that the NYPD used FRT to target Derrick Ingram for his leadership of a peaceful Black Lives Matter protest. Police later surrounded Derrick's home with more than 50 officers as part of a retaliatory raid.[27]

Because of its documented biases and its replication of historically flawed police practices, FRT should not be used by the NYPD or any other government agency. We call on the Council to introduce legislation banning all government use of FRT. In continuing to fail to act to ban the technology, New York falls further and further behind progressive cities from around the world.[28] Our coalition has been pushing these three FRT bills for over two years and it is long past time for the Council to protect New Yorkers by banning this dangerous technology.

The POST Act was a landmark bill because it reasserted the Council's indispensable role in overseeing all NYPD operations, including its use of harmful surveillance technology like FRT. The Council must reassert its authority to ensure that the bill it fought so long to implement is not totally ignored.

---

[24] Khari Johnson, *NYPD Used Facial Recognition and Pics of Woody Harrelson to Arrest a Man*, VENTUREBEAT, May 16, 2019, https://venturebeat.com/2019/05/16/nypd-used-facial-recognition-and-pics-of-woody-harrelson-to-arrest-a-man.
[25] Clare Garvie, "Garbage In, Garbage Out: Face Recognition on Flawed Data," Georgetown Law Center on Privacy and Technology, May 16, 2019, https://www.flawedfacedata.com.
[26] *Id.*
[27] George Joseph & Jake Offenhartz, *NYPD Used Facial Recognition Technology in Siege of Black Lives Matter Activist's Apartment*, GOTHAMIST, Aug. 14, 2020, https://gothamist.com/news/nypd-used-facial-recognition-unit-in-siege-of-black-lives-matter-activists-apartment.
[28] Shannon Flynn, *13 Cities Where Police Are Banned from Using Facial Recognition Tech*, INNOVATION & TECH TODAY, Nov. 18, 2020, https://innotechtoday.com/13-cities-where-police-are-banned-from-using-facial-recognition-tech; Kyle Wiggers, *AI Weekly: EU Facial Recognition Ban Highlights Need for U.S. Legislation*, VENTUREBEAT, Oct. 8, 2021, https://venturebeat.com/2021/10/08/ai-weekly-eu-facial-recognition-ban-highlights-need-for-u-s-legislation.